Institutional Repository - Research Portal
Dépôt Institutionnel - Portail de la Recherche
researchportal.unamur.be
University of Namur

RESEARCH OUTPUTS / RÉSULTATS DE RECHERCHE

Conceptualizing a Responsibility based Approach for Elaborating and Verifying RBAC Policies Conforming with CobiT Framework Requirements

Feltus, Christophe; Dubois, Eric; Petit, Michaël

Published in:
Proceedings of the Third International Workshop on Requirements Engineering and Law (RELAW10), in conjunction with RE 2010, Sydney, Australia

DOI:
10.1109/RELAW.2010.5625355

Publication date:
2010

Document Version
Early version, also known as pre-print

Link to publication

Citation for pulished version (HARVARD):
Feltus, C, Dubois, E & Petit, M 2010, Conceptualizing a Responsibility based Approach for Elaborating and Verifying RBAC Policies Conforming with CobiT Framework Requirements. in *Proceedings of the Third International Workshop on Requirements Engineering and Law (RELAW10), in conjunction with RE 2010, Sydney, Australia.* IEEE, pp. 34-43. https://doi.org/10.1109/RELAW.2010.5625355

General rights
Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal ?

Take down policy
If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

Download date: 13. Oct. 2024

Conceptualizing a Responsibility based Approach for Elaborating and Verifying RBAC Policies Conforming with CobiT Framework Requirements

Toward a Business/IT Alignment Method based on the Translation of Business to Application Roles

Christophe Feltus, Eric Dubois
Public Research Center Henri Tudor
Luxembourg-Kirchberg,
Luxembourg
christophe.feltus@tudor.lu, eric.dubois@tudor.lu

Michaël Petit
PReCISE Research Centre,
Faculty of Computer Science, University of Namur,
Belgium
mpe@info.fundp.ac.be

***Abstract*—The objective of this paper is to present the first results toward the definition of a two steps approach for aligning business level requirements issued from corporate framework such as CobiT down to technical policies such as the access rights modeled by RBAC. To achieve that, our approach is based on the concept of employees' responsibility. Using this concept is motivated by the importance and the omnipresence of the responsibility all along the company frameworks, from the CEO responsibilities such as in the financial sector as defined by Sarbanes-Oxley Act down to the responsibility at the operation layer such as the one of a trader who must follow stock quotes for private banking. The approach is illustrated based on an example, which highlights how access rights are assigned to employees having responsibilities defined at the CobiT framework layer.**

Keywords-Alignment; CobiT; Responsibility; Traceability; Access right; RBAC; Requirement engineering.

I. INTRODUCTION

In all the company's layers, standards and norms define business activities. Those activities are called strategic activities at the higher layer such as the activity to report the company's results at the board of directors, management activities at the intermediary layer like activities to manage the budget of a company unit, or operational activities at the lower layer such as the activity to encode customers' data. For all of those activities, implementation rules (e.g.: access right policies) must accordingly be defined. For instance, at the higher layer, the CEO needs to have access to strategic data to prepare the company report, at the intermediary layer, the unit managers need to have access to the accounting software to manage the budget and at the lower layer, and secretaries need access to the customer database.

Meanwhile governance standards and norms [1, 2, 3] request a strict alignment between these business layer activities and the corresponding rights. This strict alignment affords e.g. to respect the principle of least privilege and, by consequence, to provide to the employees with strict rights, which are indispensable to achieve their goals. For instance, it is not permitted to give access to the customer database to the whole team of secretaries if only one of them is concerned with the customers' records. The financial sector is particularly sensitive to this requirement and additionally requests traceability of this alignment of permission and rights according to business needs. In practice, this alignment between the business view and the technical view is problematic and the traceability of the right assigned to the employee according to the business specifications too.

In most companies, the management of employees' permissions and rights is done by using the central concept of a role, which permits to manage a large amount of users on the one hand and the permissions assigned to the role on the other hand. Role engineering is the process to define roles, which ought to be affected to a set of users who have the same function in the company. The Role Based Access Control (RBAC [4]) has emerged as a reference model in this discipline. RBAC models two main types of assignments, which are the user-role assignment and the permission-role assignment. That means that a role is defined with a set of permissions and that users are assigned to his role to get the permissions.

Using the concept of role presents weaknesses due to the difficulty to align the role defined at the business layer (business role) and at the same time the roles used at the IT layer to operate IT transactions (application role). This weakness brings out two kinds of situations. Firstly, the company restricts its number of application roles to the amount of business roles. In this first case, the company works with a limited number of roles and employees receive, by the way, more permissions and rights than they need. In the second case, the company defines as many application roles as IT transaction possibilities. In this second case, the company works with many roles, which renders the access right management difficult and decreases the advantages of according to RBAC specifications. This problem mainly emerges due to the misalignment between business role and application role. The business roles gather employees with the same function who can have different tasks to perform, although application roles gather employees with the same tasks to perform but this could be assigned to different business role.

Based on the review of the literature, we have observed that the concept of responsibility is central to the business models and that it can be model with concepts from the business view like the employee's obligations and accountabilities, and concepts from the technical view like

the employee's rights, access rights and permissions needed to perform business obligations. In previous work [5, 6], we have elaborated a responsibility meta-model (Fig. 2) built around three sets of concepts: (i) the accountability of an employee regarding an obligation derived from a responsibility; (ii) the rights required to fulfill the obligation; (iii) the commitment pledged by the employee to fulfill the obligation. Whereas the first two sets are common in the field of IT, the last one derives from social aspects, which underline the importance of dealing with the engagement of the employee in the responsibility assignment process.

In this paper, we present a responsibility centered meta-model, which permits to assure the interoperability between the business view and the technical view and we explain how it can be used as a pivot point between both. We propose a method that has the objective to assign permissions to employees and also permits to trace this assignment. This method is a two steps approach (Fig. 1). In the first step, the meta-model is mapped with CobiT (business view) and responsibilities are defined and associated to business roles issued from the business framework they refer to. In the second step, the meta-model is mapped with RBAC (technical view) and the responsibilities previously defined are assigned to employees following the RBAC model.

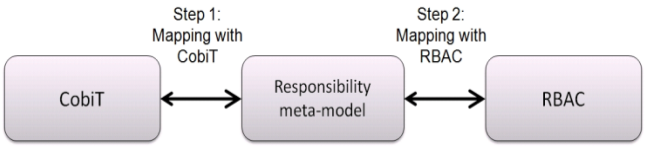

Figure 1. Two steps of the responsibility based approach

In the next section, we present the responsibility meta-model and its concepts, and propose our own definitions of them. In section III, we present the first step of the approach related to the mapping of the responsibility meta-model with CobiT. In section IV, we introduce the second step of the approach, which maps the meta-model with RBAC and considers the assignment of employees and permissions to responsibilities. In section V we conclude the paper.

II. THE RESPONSIBILITY META-MODEL

The elaboration of the responsibility meta-model (Fig. 2) has been performed based on literature overview. We have firstly analyzed how the responsibility is included in information technology professional frameworks (ISO 15504 [7], ISO 27000 [8], CIMOSA [9], ITIL [10] and COBIT [11]), in the field of requirement engineering and role engineering [12], and in the field of access control with the review of the DAC, MAC, RBAC and UCON model [13].

The literature overview has permitted to observe that some components are commonly accepted, whereas others are missing or not at all addressed by the field of IT. The stakeholder is the basic component and is most of the time associated to a group. Stakeholder appears as a person, an employee, a subject, a system or a software component. We use the term *employee* since our responsibility meta-model is more for business usage. Most of the time the responsibility also refers to a duty, which may take a large scale of representations i.e.: the performance of a scenario or the achievement of a task. We propose to refer the employee's responsibility to a behavior, which we represent by the Task performed by an Actor on an Object. Capability is a component that is part of most frameworks. Capability is most frequently declined under access right, authorizations or permissions. Obligation is a component,, which exists mainly in engineering methods and which is declined as the obligation to achieve a task or to perform an action.

Commitment does not really exist in requirement engineering but appears only punctually and not explicitly in some management frameworks like CobiT. The literature overview in the field of IT has been completed by a literature review in the field of Human Sciences. This has permitted to complete the understanding of some concepts such as concepts of commitment, commitment antecedents, accountability and sanction.

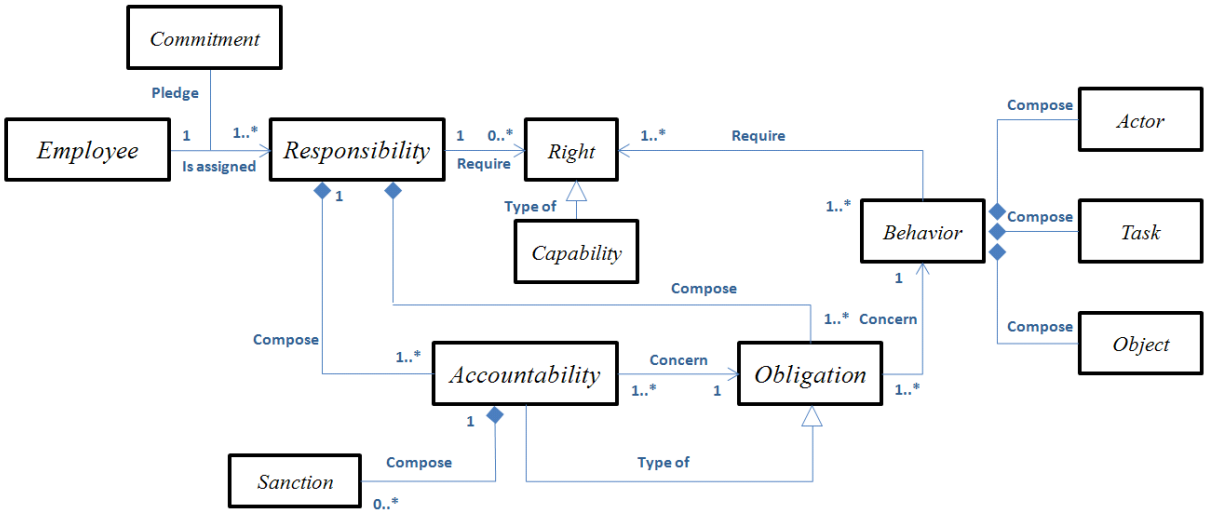

Figure 2. Responsibility meta-model UML diagram

To structure the meta-model, we define three sets of concepts: the obligation/ accountability, the right and the delegation/ assignment process.

From the literature review, we propose our own definitions of the concepts:

Responsibility	*a state assigned to an employee to signify him its obligation concerning a behavior, the accountability regarding this obligation and the right necessary to perform it*
Behavior	*a task performed or avoid by an actor with or on an object*
Task	*an action to use or transform an object*
Object	*a material or immaterial entity that can be transformed or used*
Employee	*a human actor hired in a company*
Actor	*a human or a machine that performs a task*

A. Concept of obligation/accountability

Obligation (Fig. 3) is the most frequent concept to appear as well in literature as in industrial and professional frameworks. Two types of obligations have been defined by Dobson [14]: functional obligation that points out what a role must do with respect to a state of affairs (e.g. execute an activity) and a structural (managerial) obligation that represents what a role must do in order to fulfill a responsibility such as directing, supervising and monitoring, whenever an obligation or a right is delegated.

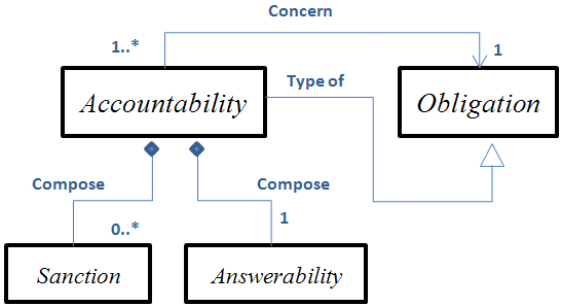

Figure 3. Obligation concept UML diagram

Accountability and Answerability are closed concepts. Both of them are types of obligations to report the achievement, maintenance or avoidance of some given state [15] to an authority. The difference between them is that one accountability is composed of one answerability and zero or many sanctions [16]. Stahl [17] argues that accountability describes the structures, which have to be in place to facilitate responsibility and that responsibility is the *ascription of an object to a subject* rendering the subject answerable for the object. Stahl also focuses on the sanction as being of central importance to responsibility. He nuances the sanction as positive or negative. The answerability is defined by Cholvy as *an obligation or a moral duty to report or explain the action or someone else's action to a given authority* [18]. There are other definitions of accountability. Laudon and Laudon [19] define this concept in the following way: *Accountability is a feature of systems and social institutions: It means that mechanisms are in place to determine who took responsibility of actions* with the following definition: *responsibility has to do with tracing the causes of actions and events, of finding out who is answerable in a given situation*. For Goodpaster and Matthews [20] accountability is a mechanism set allowing such tracing of causes, actions, and events, whereas for Spinello [21], it is a necessary but not a sufficient responsibility condition.

We propose the following definitions of the concepts introduced in the meta-model:

Answerability	*a state assigned to an employee which could justify the performance of a behavior to someone else*
Sanction	*a task or an object gained by the employee resulting of the performance of an accountability*
Accountability	*a type of obligation to justify the performance of a behavior to someone else under threat of sanction*
Obligation	*a type of behavior that links a responsibility with a behavior that must be performed*

B. Concept of right

The concept of right (Fig. 4.) is common but is not systematically embedded in the frameworks. It encompasses facilities required by an employee to fulfill his obligations.

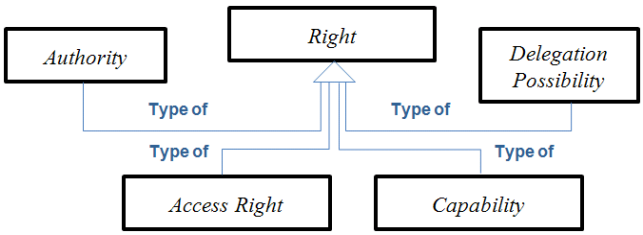

Figure 4. Right concept UML diagram

Capability describes the requisite qualities, skills or resources necessary to perform an action. Capability is a component,, which is part of all models and methods [9, 15, 22], and it may be declined through knowledge or know-how needed by the employee, but also time, training, manpower, budget, material, etc.

Authority describes the power or right to give orders or to make decisions. This concept is introduced in CIMOSA [9] as the *power* to command and control other employees and to assign responsibilities. CIMOSA argues that responsible employees have rights over resource in the first place and over process, action and task in the second place. CIMOSA distinguishes resources from their capabilities: Resources are companies' assets required for carrying out processes, whereas capabilities are technical abilities provided by a specific resource. There are four types: functional, performance, object oriented or operational.

Delegation right describes the right to transfer a part of the responsibility to another employee who pledges commitment for it (Cf. next section). This transfer may concern the transfer of rights, of obligations or of both. The delegation of an obligation may or may not be accompanied

by the delegation of the right to further delegate this same obligation [15]. This delegation of rights depends on the right's type (access to information, money, time…) and on the employee's status, function or position. This delegation also may or may not include the transfer of obligation as the obligation to be accountable [23].

We propose the following definitions of the concepts introduced in the meta-model:

Right	*a facility required to perform a behavior*
Delegation Possibility	*the right to delegate all or some part of the responsibility to another employee*
Authority	*the power or right to give orders or make decisions (from CIMOSA)*
Access Right	*the right to access an object*
Capability	*employee qualities, skills or resources*

C. *Assignment/delegation process*

Assignment is the action of linking an employee to a responsibility and delegation process is the transfer of an employee's responsibility assignment to another employee.

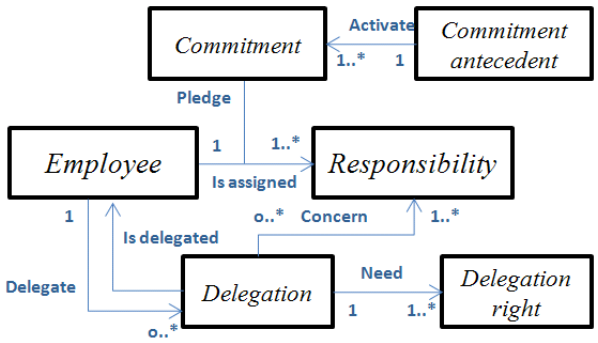

Figure 5. Assignment/delegation process UML diagram

The commitment pledged by the employee related to this assignment or delegation process represents his moral engagement to fulfill the action and the assurance that he does it in respect of an ethical code. The commitment remains a virtual concept, difficult to define as well as to integrate in a strictly formalized framework. In [24], Meyer and Allen acknowledge that *commitment should be conceptualized as a psychological state concerned with how people feel about their organizational engagements*. To bypass the integration difficulty, we propose to integrate the components, which enforce the commitment, as an alternative solution into the meta-model. These components, traditionally called *Commitment's antecedent* in literature, correspond to more pragmatic variables [25] (Fig. 5).

The antecedents may take many forms depending on the type of commitment. These forms are i.e. the characteristics and the experiences a person brings to the organization [26], the employee's age and the time he is part of the organization [27, 28, 29], the perception of job security [30], the management culture and style [31], the employee's investments in time, money and effort [32]. A scientific survey of the commitment also highlights that *Commitment outcomes* may really influence the quality and efficiency of the action achieved. Pfeffer explains in [33] that *Employee commitment is argued to be critical to contemporary organizational success*. The following list summarizes commitment outcomes:

- The employee performance [34]. Committed employees performed better because of their high expectations of their performance. Moreover, employees have a high level of performance when they are committed to both, their organization and their profession.
- The retention of the employee. Many studies reveal a link between the employee's commitment and his turnover [32, 34, 35].
- The citizen behavior or extra-role behavior. The research on these outcomes remain however inconclusive [36].

Based upon the commitment outcomes and antecedent definition, we may assume that being committed to the responsibility of an action for an employee on the one hand means an increasing of trust in the achievement of the obligation or in the accountability attached to responsibility, and on the other hand more efficiency (and consequently more capabilities) for this employee to perform the action.

We propose the following definitions of the concepts introduced in the meta-model:

Commitment	*a state of being of an employee who pledges a personal engagement to perform a behavior*
Commitment Antecedant	*a state or behavior that brings about commitment*
Commitment Outcomes	*a state or behavior that results in employee commitment*

III. STEP 1: BUILDING RESPONSIBILITIES

The first step of the approach consists of building the responsibilities by mapping the responsibility meta-model with the CobiT framework.

A. *Responsibility in CobiT*

The CobiT responsibility model is formalized through a RACI chart matrix attached to all 34 CobiT processes. RACI stands for Responsible, Accountable, Consulted and Informed and defines what the responsibilities of the business roles must be, regarding the key activities of control. CobiT addresses the responsibility of all business roles assigned to employees involved in IT governance and IT security actions.

The paper is illustrated based on the AI6 control of CobiT: *Manage Change*. CobiT provides a framework for controls without providing fine grain tuning rights and obligations of each business roles on this control. Indeed, if we look at the *Manage Change* control, we observe that one CobiT control provides: a process description, control objectives, a list of inputs, a list of outputs, a list of activities

and their corresponding RACI charts, goals and metrics, and a maturity model. CobiT's objective is to provide control requirements and guidelines for deploying those controls in practice. As a consequence, the framework does not provide detailed information to deploy the standard in practice and additional information needs to be engineered in the company itself. For instance, CobiT provides 8 business roles involved in the *Manage Change* process (Fig. 4): *CIO, Business Process Owner, Head of Operations, Chief Architect, Head Development, Head IT Administration, PMO and Compliance, Audit, Risk and Security*. Each of those business roles may be affected by up to 5 activities, and have different functions (R, A, C, I) through those activities. In this case, we have got 8 business roles X 5 activities X 4 functions = 160 possible assignments. In the rest of the paper, we consider and call the RACI functions responsibilities. As consequence, employees may be assigned to the responsibility to be accountable, to be responsible, to be informed and to be consulted. By the mean time, it is unrealistic to provide the same rights and same obligations to all employees. For instance, the *Head Operation*, which is responsible and accountable for *Authorizing changes*, does not have the same rights and obligations that the *Business Process Owner* which is informed of *The management and dissemination of relevant information by regarding the changes*. In practice, deploying CobiT in the company implies to precise what the responsibilities of each employee for all controls are and to ensure that those responsibilities are personally accepted.

B. *Alignment of the responsibility meta-model with CobiT responsibilities*

The mapping of CobiT and the responsibility meta-model (Fig. 7) permits to instantiate the meta-model with inputs from CobiT. In this figure, we observe that:

- the 4 responsibilities (R, A, C, I) from the RACI chart correspond to four types of responsibilities taken from the responsibility meta-model,
- the obligations, which combine responsibility and rights require are provided by the CobiT Framework,
- the RACI chart is provided by the CobiT framework, is composed of responsibility, business role, and activity,
- CobiT assignment of business role to employee makes the link between the employee and CobiT obligations and rights,
- Activity is composed of tasks, which may partially be extracted from CobiT.

If we consider AI6 control of CobiT: *Manage Change*, this control is composed of five activities (Fig. 6):

1. *Develop and Implement a process to consistently record, assess and prioritise change requests,*
2. *Assess impact and prioritise changes based on business needs,*
3. *Assure that any emergency and critical change follows the approved process,*
4. *Authorise changes,*
5. *Manage and disseminate relevant information regarding changes.*

Activities \ Functions	CEO	CFO	Business Executive	CIO	Business Process Owner	Head Operations	Chief Architect	Head Development	Head IT Administration	PMO	Compliance, Audit, Risk and Security
Develop and implement a process to consistently record, assess and prioritise change requests.				A	I	R	C	R	C	C	C
Assess impact and prioritise changes based on business needs.				I	R	A/R	C	R	C	R	C
Assure that any emergency and critical change follows the approved process.				I	I	A/R	I	R			C
Authorise changes.				I	C	A/R		R			
Manage and disseminate relevant information regarding changes.				A	I	R	C	R	I	R	C

Figure 6. *Manage Change* control RACI chart

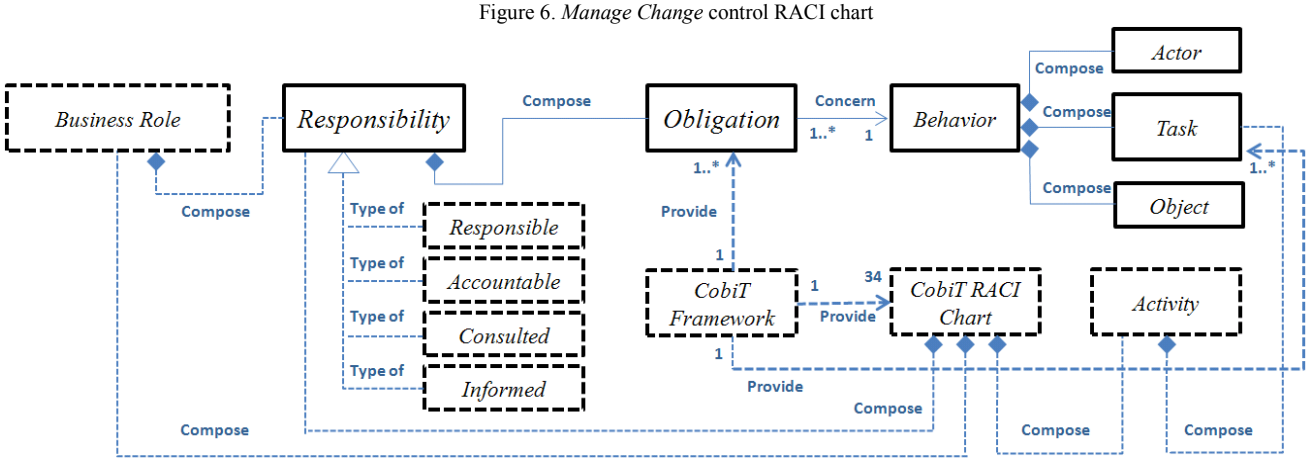

Figure 7. Mapping responsibility and RACI chart UML diagram

The deeper analysis of the second activity of control *Assess impact and priorities change based on business needs* highlights that eight business roles are susceptible, according to CobiT, to be assigned to the four RACI responsibilities:

- Accountable: *Head operation*
- Responsible: *BPO, PMO, Head operation, Head development*
- Consulted: *Chief Architect, Head IT operation and Compliance, Audit, Risk and Security*
- Informed: *CIO*

Suppose the responsibility of being responsible. The meaning for CobiT's responsibility is the employee who gets the action done. This responsibility is spread over 4 business roles but CobiT does not provide more information which tasks of these activities are being achieved by which employee, neither by which business role. To instantiate the responsibility meta-model, we need to collect all the tasks, which compose the activity and associate them with the business role foreseen for this responsibility. This association is obtained by analyzing the company's processes or usual practices. Those tasks are partially provided by CobiT and are completed with data from other frameworks such as ITIL or from company's specific data and practices (Table I).

TABLE I. RACI RESPONSIBILITIES TO TASKS ASSOCIATION

From CobiT:

Tasks	Resp.
Assessing change (based on business needs)	R
Priorising changes (based on business needs)	R
Assess the impact of change to the IT infrastructure, application and technical solutions	R
Scheduling change	R

From ITIL:

Be available for consultation should an urgent Change required	C
Attend all relevant CAB (Change Advisory Board)	A
Consider all changes on the agenda and give an opinion on which changes should be authorized	A

From the company:

Inform about the Business needs	C
Perform a monthly review	A
Introduce changes scheduled in a database	R
Prepare CAB report	A
Accountability concerning "Priorising changes" : Justify the priorising	A
The CAB is informed about the changes	I

The activity *Assess impact and prioritize changes based on business needs* is composed of obligations to realize tasks. Those tasks are afterward mapped to a kind of responsibility corresponding to the RACI chart. The association of RACI responsibility to tasks is based on the CobiT definitions of responsibility: R is *the employee who gets the action done* and corresponds the following tasks, e.g.: *assessing change*, *prioritizing changes*, *scheduling change*, etc. A is *the employee, who provides direction and authorizes an action* and corresponds the following tasks , e.g.: *Attend all relevant CAB*, *Consider all changes on the agenda and give an opinion on which changes should be authorized,* etc.

After the mapping with CobiT and the responsibility meta-model, we have got a list of tasks, which composes each activity and, through the RACI chart, a list of business roles, which can be assigned responsible for all those tasks. For instance the responsibility to *Schedule change* can be assigned in the step 2 of the approach to employees who have one of the following business roles: *BPO, PMO, Head operation, Head development.*

C. Right to Task association

In order to provide the strictly necessary permissions and rights requested to perform a task to a responsibility, we have to directly link the concept of right to the concept of responsibility rather than to the concept of business roles.

To instantiate the concept of rights, we analyze task by task which rights and permissions are indispensible to perform those tasks.

TABLE II. RIGHTS TO TASKS ASSOCIATION

From CobiT:

Tasks	Rights
Assessing change (based on business needs)	*List of required changes (CobiT), information related to the business needs*
Priorising changes (based on business needs)	*List of accepted changes, information related to the business needs*
Assess the impact of change to the IT infrastructure, application and technical solutions	*List of required changes (CobiT), documentation related to the IT infrastructure, List of applications and technical solutions*
Scheduling change	*List of required changes (CobiT), List of accepted changes, list of priorising changes*

From ITIL:

Be available for consultation should an urgent Change required	*List of urgent required changes*
Attend all relevant CAB (Change Advisory Board)	*No right*
Consider all changes on the agenda and give an opinion on which changes should be authorized	*List of required changes (CobiT)*

From the company:

Inform about the Business needs	*Management report*
Perform a monthly review	*List of required changes (CobiT), List of accepted changes*
Introduce changes scheduled in a database	*List of accepted changes*
Prepare CAB report	*List of required changes (CobiT), List of accepted changes*
Accountability concerning "Priorising changes" : Justify the priorising	*List of changes schedules and justifications*
The CAB is informed about the changes	*List of required changes (CobiT), List of accepted changes, list of priorising changes*

For AI6 control, the rights and permissions do not exist explicitly in CobiT but some first information is provided by the inputs indispensible for the control. Those control inputs however do not separately target each task of the control but the control as a whole. These rights are also not refined according to one type of responsibility (R, A, C, I). By consequence, the required rights are extracted from a fine grain analysis of CobiT, completed with such a fine analysis of ITIL and, for illustration, with some rights, which are issued from the company's business processes as well. For this example, those rights are fictitious and for illustration only.

IV. STEP 2: ASSIGNING RESPONSIBILITIES

The second step of the approach consists of modeling the assignment of permissions to employees by mapping the responsibility meta-model with RBAC model.

A. RBAC User-Role and Permission-Role assignment process

The concept of role has been introduced to software engineering about 35 years ago and has followed the development of traditional access control techniques such as the Mandatory Access Control or Discretionary Access Control. Role Based Access Control (Fig. 8) has been introduced in the NIST standard for role-based access control [4] and embodies the entire previously developed notions in a single model which is now the reference access control mechanism for most software applications. The publication of this standard has been followed by many related papers which adapt the model for specific fields (e.g. eCommerce, [37]), to propose alternative solutions according to other constraints (Context Aware RBAC, [38]), or to propose solutions for managing some of its aspects (e.g. ARBAC [39], URA97 [40] or PRA97 [41].

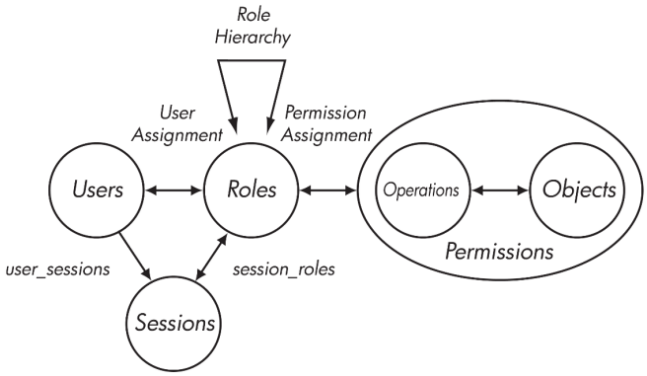

Figure 8. RBAC model

RBAC is a high level model with the objective to simplify the management of granting permissions to users. This is especially necessary in multinational companies where the amount of employees often count in thousands. It provides access decisions based on two associations – the association of users to roles based on the function that users assume, and based on their responsibilities, and the association of permission to roles describing that a role has the permission to perform specific operations on objects. This means that it is easy to change the assignment of people to roles without changing permissions. RBAC is a high level model with the objective to simplify the management of granting permissions to users. This is especially necessary in multinational companies where you have thousands of employees. It provides access decisions based on two associations – the association of users to roles based on the function, which users assume and based on their responsibilities, and the association of permissions to roles describing that a role has the permission to perform specific operations on objects. This means that it is easy to change the assignment of people to roles without changing permissions.

The process to assign users to roles and permissions to roles is normally a managerial function performed by the business manager or the process owner to decide which employee needs to access what application to achieve her job. The actual implementation may be delegated by the application business owner to a security administrator. URA97 [40] and PRA97 [41] are both part of the ARBAC97 [39] model (Administrative RBAC), which permits the assignment of the users to roles and permission to role by means of administrative roles and permissions. Both URA97 and PRA97 are defined in the context of RBAC96 model family but are applicable for most of the RBAC model. Their philosophy is to create of administrative roles managed by security officers. These administrative roles are granted administrative permissions to assign or to remove users to/from roles. In the same way that RBAC96 defines role hierarchies, ARBAC97 defines administrative role hierarchy, so that a senior security officer inherits permissions from a junior security officer below him in the role hierarchy. For example, if the junior has assigned an employee to an inappropriate business role, the senior security officer can remove this employee from the role or change the permissions associated with it. URA97 gives a detailed explanation of the administration of the assignment process.

B. Employee-Responsibility assignment process based on RBAC

To capitalize on the advantages of RBAC for managing access rights, needed by employees to perform a task (Table II), we could consider the business role defined by CobiT as the RBAC concept of role (which we call application role), and associate employees and permissions to this application role. The problem by doing so, is that the activities are composed of tasks and that all of the employees, who are assigned to a business role, do not have to achieve all tasks targeted by this business role. By consequence, doing that would provide some employees with too many permissions and would be in opposition to the minimum of privilege principle.

To face this problem, we propose to map the responsibility concept with the RBAC concept of role (application role) and consider those responsibilities as types of application roles. Additionally, we consider the employee corresponding to the RBAC concept of a user and that the rights assigned to the responsibilities correspond to the RBAC concept of permission (Fig. 9).

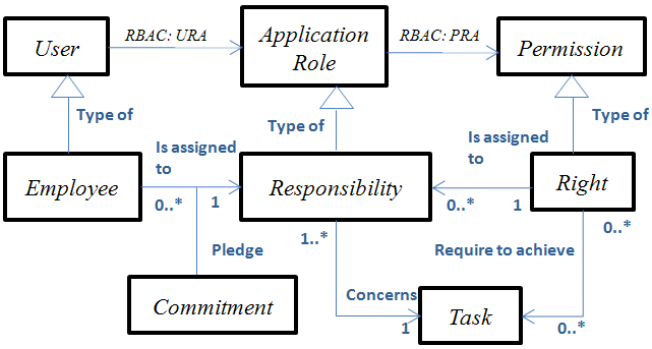

Figure 9. Mapping responsibility and RBAC UML diagram

The mapping of the responsibility meta-model achieved in step 1, has permitted to instantiate the concepts of activity, task, responsibility and right. From the mapping of RBAC with the responsibility meta-model achieved in step 2, we have modeled the assignment of permissions to employees by the intermediary concept of responsibilities.

C. *Employee commitment to the responsibility*

According to the previous section, we agree upon the idea that the simplest way for a manager to assign permissions to an employee is to *simply* assign this employee to a responsibility, which encompasses specific tasks to perform and is associated to the permissions needed to perform the tasks. By doing so, the manager implicitly obliges the employee to accept the responsibility to perform the tasks, but he does not actually know whether the employee has agreed to this. Not taking the employee's commitment into account is an authoritarian way of managing the staff and may result in company goals not being achieved due to unwillingness of employees to perform assigned tasks (see section II.*D*). Although this may seem unavoidable, especially in large companies, it could easily be improved by incorporating acceptance of responsibility by an employee within the responsibility assignment process.

In order to explain how the commitment may be included in the employee to responsibility assignment process, a conceptual assignment process is proposed as illustrated in Fig. 9. When being assigned to a responsibility, the employee needs to explicitly commit to the achievement of the task(s) related to the responsibility. This concept of commitment does not exist in RBAC as it considers the assignment of an employee to a role as an action performed solely by the employee's manager. Based on our review of the significance of the commitment in section II.*D* and according to the responsibility meta-model, we propose to integrate the commitment to the employee to responsibility assignment process.

An employee responsibility assignment process may start with a request from a delegator to transfer the obligation related to a task to an employee (Fig. 10). This transfer is possible if the employee's manager accepts the assignment of the responsibility to the employee and if this employee explicitly commits to fulfill the task. The first condition corresponds to a double control: the employee's availability and the employee's capability. In some cases, the employee is also the manager and consequently, decides whether to accept or reject new responsibilities according to availabilities. The second condition corresponds to the commitment pledged by the employee according to his perception of the environment, guarantees received, interest in the task, etc. (see commitment antecedent in section II.*D*).

Once the delegator receives the agreement from the employee's manager and the commitment from the employee, the delegator requests the RBAC administrator to provide the permissions needed to achieve the task. As soon as the permissions are granted, the employee is assigned to the responsibility (Fig 10).

D. *Example of assignment process*

To assign an employee responsible for the task *Prioritizing changes (based on business needs)*, which compose the activity *Assess impact and prioritize changes based on business needs,* we firstly have to identify to which responsibility this task is corresponding. According to Table I, we see that it corresponds to the responsibility to be responsible and that this responsibility is assigned to the four following business roles: *BPO, PMO, Head operation, Head development* (Fig. 6).

Suppose that Bob is a *Business Process Owner (BPO)* who is considered interesting by the CobiT Manager to be assigned to this responsibility. Before the assignment, Alice who Bob's manager has to check e.g.: that Bob has enough capabilities to achieve the work and that he is available as well. Additionally, that new responsibility is proposed to Bob who has to commit to it. Once Bob is committed and if Alice has confirmed Bob's capability and availability, the RBAC administrator has to assign Bob to the application role, which corresponds to this responsibility and that is assigned the corresponding access rights, according to Table II:

- *List of accepted changes*,
- *Information related to the business needs*

V. Conclusion

In this paper, we propose a conceptualizing responsibility based approach for elaborating RBAC policies conforming to CobiT requirements. The objective of the approach is to improve the assignation of permissions to employees and to permit by the mean time to trace this assignment. The centric component of the approach is the responsibility of the employees, which is used as a pivot point between the business view and the IT view.

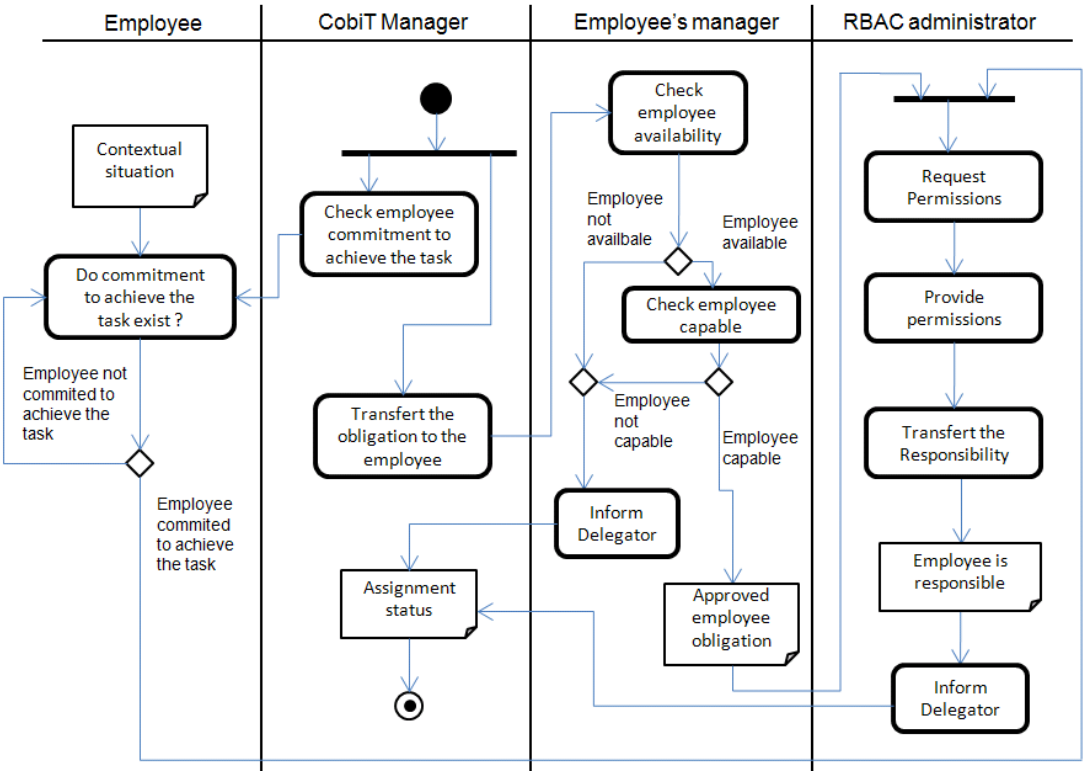

Figure 10. Workflow for assigning responsibility taking into account employees' commitment

Although the business role aims to gather a number of employees with the same functions under the same set, that business role cannot directly be mapped to application roles. We propose to use the concept of responsibility as hyphens between both types of roles. Responsibility refers in its definition to the employees' obligations, required rights by this obligation and their personal engagement to fulfill this obligation. This perception of responsibility, by the way, is that it does not attempt to replace the role or to be a subset of it, but rather, has for finality to refine the link between an employee, its business obligations, and its IT rights and permissions.

The approach is structured in 2 steps:

1. The mapping of the responsibility meta-model with the CobiT framework , which permits to decompose CobiT activities on tasks, map RACI responsibility to these tasks and define the requisite right to perform the task.
2. The mapping of the responsibility meta-model with RBAC has permitted to model the assignment of permissions to employees by the intermediary concept of responsibilities and has permitted to assign employees to responsibilities taking the employees' commitment into account.

The approach has been illustrated based on Bob's responsibility to be responsible. This responsibility also includes following the responsibility meta-model, an accountability which is defined by the obligation to report the achievement of a task and as such, is a task itself, which requests additional permissions to be assigned to Bob such as: access to the reporting tool.

Although the responsibility as been used in this paper as a vector to aligned business roles with application roles in an access right policy engineering process, it could also have been used to control the assignment of permissions to employees in a situation in production. This would have been achieved by analyzing if the permissions requested to perform an activity would be dully assigned to an employee, himself assigned to a business role with responsibility over this activity.

ACKNOWLEDGMENT

This research was funded by the National Research Fund of Luxemburg in the context of TITAN (Trust-Assurance for Critical Infrastructures in Multi-Agents Environments, FNR CO/08/IS/21) project.

REFERENCES

[1] ISO/IEC 38500 (2008), International Standard for Corporate Governance of IT.

[2] P. S. Sarbanes, and M. Oxley (2002) Sarbanes-Oxley Act of 2002.

[3] Basel Committee on Banking Supervision, International convergence of capital measurement and capital standards; BIS; Basel, June 2004.

[4] D. F. Ferraiolo, R. Sandhu, S. Gavrila, D. R. Kuhn, and R. Chandramouli. 2001. "Proposed NIST standard for role-based access control". ACM Trans. Inf. Syst. Secur. 4, 3 (Aug. 2001), 224-274.

[5] C. Feltus, M. Petit, and M. Sloman, "Enhancement of Business IT Alignment by Including Responsibility Components in RBAC", Proc.

5th International Workshop on Business/IT Alignment and Interoperability (BUSITAL 2010), Hammamet, Tunisia.

[6] C. Feltus, M. Petit, and E. Dubois, "Strengthening employee's responsibility to enhance governance of IT: COBIT RACI chart case study". Proc. of the First ACM Workshop on Information Security Governance. ACM, New York, NY, 23-3. DOI= http://doi.acm.org/10.1145/1655168.1655174.

[7] ISO/IEC 15504, Information Technology – Process assessment, (parts 1-5), 2003-2006.

[8] ISO/IEC 27001:2005, "Information technology – Security techniques – Information security management systems – Requirements", 2005-10-15.

[9] F. B. Vernadat, "Enterprise Modelling and Integration", Chapman & Hall, London (1995), ISBN 0-412-60550-3.

[10] ITIL (2001), IT Infrastructure Library – Service Delivery, The Stationery Office Edition, ISBN 011 3308930.

[11] COBIT 4.1, Control Objectives for Information and Related Technology, Information Systems Audit and Control Association..

[12] C. Feltus, and M. Petit, "Building a Responsibility Model Including Accountability, Capability and Commitment" 4th International Conference on Availability, Reliability and Security (ARES), 2009, Fukuoka, Japan .

[13] R. Sandhu, and J. Park, "Usage Control: A Vision for Next Generation Access Control", Proc. of the Second International Workshop on Mathematical Methods, Models and Architectures for Computer Networks Security, 2003.

[14] J. Dobson, and D. Martin, "Enterprise Modeling Based on Responsibility, Trust in Technology: A Socio-Technical Perspective", Clarke, K., Hardstone, G., Rouncefield, M. and Sommerville, I., eds., Springer, 2006.

[15] I. Sommerville, R. Lock, T. Storer, and J. Dobson, "Deriving Information Requirements from Responsibility Models", Proc. of the 21st International Conference, CAiSE 2009, Amsterdam, The Netherlands, June 8-12, 2009. ISBN 978-3-642-02143-5.

[16] J. A. Fox, "The uncertain relationship between transparency and accountability" (August 1, 2007). Center for Global, International and Regional Studies. Reprint Series. Paper CGIRS-Reprint-2007-2. http://repositories.cdlib.org/cgirs/reprint/CGIRS-Reprint-2007-2.

[17] B. C. Stahl, "Accountability and reflective responsibility in information systems". In: C. Zielinski et al. The information society - emerging landscapes. Springer, 2006, pp. 51 -68.

[18] L. Cholvy, F. Cuppens, and C. Saurel, "Towards a logical formalization of responsibility", Proc. of the 6th International Conference on Artificial Intelligence and Law, pp. 233-242, 1997.

[19] K. C. Laudon, and J. P. Laudon, "Essentials of Management Information Systems", 4th edition London et al., 1999, Prentics Hall.

[20] K. E. Goodpaster, and J. B. Jr. Matthews, "Can a corporation have a moral conscience ?" Hardvard Business Review (Jan-Feb 1982), pp. 132 – 141.

[21] R. Spinello, "Case studies in information and computer ethics", Upper Saddle River, 1997, NJ: Prentice Hall.

[22] E. S. Yu, and L. Liu, "Modelling Trust for System Design Using the i* Strategic Actors Framework." Workshop on Deception, Fraud, and Trust in Agent Societies Held During the Autonomous, Eds. Lecture Notes In Computer Science, vol. 2246. Springer-Verlag, 2001. London, 175-194.

[23] T. J. Norman, and C. Reed, "Delegation and Responsibility". In Proceedings of the 7th international Workshop on intelligent Employees Vii. Employee theories Architectures and Languages (July 07 - 09, 2000). C. Castelfranchi and Y. Lespérance, Eds. Lecture Notes In Computer Science, vol. 1986. Springer-Verlag, London, 136-149.

[24] J. P. Meyer, and N. J. Allen, 'A three component conceptualization of organizational commitment'. Human Resource Management Review. 1991. 1, 61-98.

[25] C. Vandenberghe, K. Bentein, and F. Stinglhamber, "Affective commitment to the organization, supervisor, and work group: Antecedents and outcomes", Journal of Vocational Behavior, Volume 64, Issue 1, February 2004, pp. 47-71.

[26] R. T. Mowday, L. W. Porter, and R. M. Steers, "Employee-Organization Linkages: The Psychology of Commitment", Absenteeim, and Turnover. 1982. New York: Academic Press.

[27] B. Buchanana, "Building organizational Commitment: The Socialization of Managers in work organizations", Administrative science Quarterly, 19, pp. 533 – 546.

[28] D. Hall, "Organizational Identification as a function of Career Pattern and Organizational Type", Administrative Science Quarterly, 1977, 17, pp. 340 – 350.

[29] K. Lio, "Professional Orientation and Organizational Commitment among Employees: an Empirical Study of Detention Workers", Journal of Public Administration Research and Theory, 1995, 5, pp. 231 – 246.

[30] B. P. Niehoff, C. A. Enz, and R. .A., Grover, "The Impact of Top-Management Ctions on Employee Attitudes and Perceptions", Group & Organization Studies, 1990, 15, 3, 337 – 352.

[31] G. Florkowski, and M. Schuster, "Support for Profit Sharing and Organizational Commitment: A Path Analysis", Human Relations, 1992, 45, 5, pp. 507 – 523.

[32] G. J. Blau, "The measurmement and Prediction of Career Commitment", Journal of Occupational Psychology, 1985, 58, pp. 277 – 288.

[33] J. Pfeffer, (1998). "The Human Equation". Boston, MA., Harvard Business School Press.

[34] J. P. Meyer, and N. J. Allen, "Testing the 'Side-Bet Theory' of Organizational Commitment: Some Methodological Considerations", Journal of Applied Psychology, 1994, 69, pp. 372 – 378.

[35] L. W. Porter, R. M. Steers, R. T. Mowday, and P. V. Boulian, "Organizational Commitment, Job Satisfaction, and Turnover Among Psychiatric Technicians", Journal of Applied Psychology, 1974, 59, pp. 603 – 9.

[36] E. S. Williams, K. V. Rondeau, and L. H. Francescutti, "Impact of culture on commitment, satisfaction, and extra-role behaviors among Canadian ER physicians", Leadership in Health Services, 2007, vol. 20, Issue 3, 147-158.

[37] C. Yang, "Designing secure e-commerce with role-based access control". Int. J. Web Eng. Technol. 2007, 3, 1, pp. 73-95.

[38] D. Kulkarni, and A. Tripathi, "Context-aware role-based access control in pervasive computing systems". Proc. of the 13th ACM Symposium on Access Control Models and Technologies (Estes Park, CO, USA, June 11 - 13, 2008). SACMAT '08. ACM, New York, NY, 113-122.

[39] R. S. Sandhu, V. Bhamidipati, and Q. Munawer, "The ARBAC97 Model for Role-Based Administration of Roles", Proc. of TISSEC, 1999.

[40] R. S. Sandhu and V. Bhamidipati, "The URA97 Model for Role-Based User-Role Assignment". Proc. of the IFIP Tc11 Wg11.3 Eleventh international Conference on Database Securty Xi: Status and Prospects (August 10 - 13, 1997). T. Y. Lin and S. Qian, Eds. IFIP Conference Proceedings, vol. 113. Chapman & Hall Ltd., London, UK, 262-275.

[41] R. S. Sandhu, and V. Bhamidipati, 1998. "An Oracle implementation of the PRA97 model for permission-role assignment". Proc. of the Third ACM Workshop on Role-Based Access Control (Fairfax, Virginia, United States, October 22 - 23, 1998). RBAC '98. ACM, New York, NY, 13-21.